Math. Z. (2013) 273:539–546
DOI 10.1007/s00209-012-1018-8

Mathematische Zeitschrift

Coinvariants and the regular representation of a cyclic P-group

Müfit Sezer

Received: 2 October 2011 / Accepted: 24 February 2012 / Published online: 31 March 2012

Abstract We consider an indecomposable representation of a cyclic p-group $\mathbf{Z}_{p^r}$ over a field of characteristic p. We show that the top degree of the corresponding ring of coinvariants is less than $\frac{(r^2+3r)p^r}{2}$. This bound also applies to the degrees of the generators for the invariant ring of the regular representation.

Keywords Coinvariants · Modular cyclic groups · Degree bounds

Mathematics Subject Classification 13A50

1 Introduction

Let V denote a finite dimensional representation of a finite group G over a field F. The induced action on the dual space V^* extends to the symmetric algebra $S(V^*)$ of polynomial functions on V which we denote by $F[V]$. The action of $g \in G$ on $f \in F[V]$ is given by $(gf)(v) = f(g^{-1}v)$ for $v \in V$. The ring of invariant polynomials

$$F[V]^G = \{f \in F[V] \mid g(f) = f \ \forall g \in G\}$$

is a graded, finitely generated subalgebra. A classical problem is to determine $F[V]^G$ by describing generators and relations for a given representation. An important related aspect of a representation is its Noether number, denoted by $\beta(V)$, which is defined to be least integer d such that $F[V]^G$ is generated by homogeneous elements of degree less than or equal to d. A classical theorem of Noether [12] states that $\beta(V) \leq |G|$ whenever F has characteristic zero. This result has been generalized to all non-modular characteristics ($|G| \in F^*$) by Fleischmann [8] and Fogarty [10]. Knowing the Noether number is extremely useful for

The author is partially supported by Tübitak-Tbag/109T384 and Tüba-Gebip/2010.

M. Sezer (✉)
Department of Mathematics, Bilkent University, Ankara 06800, Turkey
e-mail: sezer@fen.bilkent.edu.tr

computing a generating set because then the problem is reduced to finding invariants in a finite dimensional vector space. Unfortunately, as first observed by Richman [13], in the modular case ($|G|$ is divisible by the characteristic of F) there is no bound that depends only on the group order. In fact, Symonds [17] has recently established that $\beta(V) \leq \max\{(\dim V)(|G|-1), |G|\}$ for any representation V of any group G. Hence the Noether number is often much bigger than the group order, and even worse, the degrees of the generators increase unboundedly as the dimension of the representation increases. It is perhaps not surprising then, that the invariant ring is difficult to obtain even in the basic modular cases: Consider a representation of a cyclic p-group $\boldsymbol{Z}_{p^r}$ over a field of characteristic p. Up to a change of basis, a generator of the group acts by a sum of Jordan blocks of sizes at most p^r. Although the action is that easy to describe, an explicit generating set for $F[V]^{\boldsymbol{Z}_{p^r}}$ is known only for a handful of cases. For $r = 1$ this rather short list consists of indecomposable representations up to dimension nine and decomposable ones where each indecomposable summand has dimension at most four, see for instance [1,2,4,5,14] and [18] for a selection of cases. For $r = 2$, Shank and Wehlau [16] give a generating set for the invariants of the $p+1$ dimensional indecomposable representation. To the best of our information, no explicit description of a generating set exists for the invariants of any other faithful representation of $\boldsymbol{Z}_{p^r}$. Nevertheless, $\beta(V)$ has been computed for every representation of $\boldsymbol{Z}_p$ in [7]. It is in fact $2p-3$ for an indecomposable representation V with $\dim(V) \geq 4$. Also in [11], an upper bound for $\beta(V)$ that applies to all indecomposable representations of $\boldsymbol{Z}_{p^2}$ is obtained. This bound, as a polynomial in p, is of degree two. Based on these results for $r = 1, 2$, it is conjectured in [11, Conjecture 10] that $\beta(V)$ of a modular indecomposable representation V of $\boldsymbol{Z}_{p^r}$ is bounded above by a polynomial of degree r in p. Note that the bound in this conjecture is a substantial improvement of the bound in Symonds's theorem which gives a polynomial of degree $2r$ in p for this situation. This paper goes in the direction of providing more ground for this conjecture and establishes it for the special case of regular representations.

The Hilbert ideal, denoted by $F[V]_+^G \cdot F[V]$ is the ideal in $F[V]$ generated by invariants of positive degree. The ring of coinvariants $F[V]_G := F[V]/F[V]_+^G \cdot F[V]$ is a finite dimensional vector space. Let $\operatorname{Im}\operatorname{Tr}^G$ denote the image of the transfer map $\operatorname{Tr}^G : F[V] \to F[V]^G$ given by $\operatorname{Tr}^G(f) = \sum_{g \in G} g(f)$. Since the map Tr^G is $F[V]^G$-linear, it maps a vector space basis for $F[V]_G$ to a generating set for $\operatorname{Im}\operatorname{Tr}^G$. Therefore an upper bound for the top degree of $F[V]_G$ is also an upper bound for the degree of an element in $\operatorname{Im}\operatorname{Tr}^G$ that can not be obtained by invariants of strictly smaller degree. For this reason bounding the top degree of $F[V]_{\boldsymbol{Z}_p}$ and $F[V]_{\boldsymbol{Z}_{p^2}}$ has a crucial role in proving the bounds on Noether numbers in [7] and [11]. This paper is initiated by observing that the polynomials that are used to squeeze the top degree of $F[V]_{\boldsymbol{Z}_p}$ and $F[V]_{\boldsymbol{Z}_{p^2}}$ can be extended to the general $\boldsymbol{Z}_{p^r}$ case by considering arrays of orbit products with respect to the subgroups of $\boldsymbol{Z}_{p^r}$, rather than considering just monomials, and then by applying the corresponding relative transfers. Most of our work in this paper is devoted to the computation of the leading monomials of these generalized polynomials. We obtain that the top degree of $F[V]_{\boldsymbol{Z}_{p^r}}$ is at most $\frac{(r^2+3r)p^r}{2}$ for a modular indecomposable representation of $\boldsymbol{Z}_{p^r}$, see Theorem 5. On the other hand a result of Fleischmann et. al. [9] states that the invariants of the modular regular representation of $\boldsymbol{Z}_{p^r}$ modulo the ideal $\operatorname{Im}\operatorname{Tr}^{\boldsymbol{Z}_{p^r}}$ is (up to a scaling) the invariant ring of the regular representation of $\boldsymbol{Z}_{p^{r-1}}$. Therefore the bound for the top degree of coinvariants is quickly seen to bound the Noether number of the regular representation as well, see Corollary 6. Finally, we point out that this provides further support for [11, Conjecture 10]: In [15] it is shown that the Noether number of a modular representation of $\boldsymbol{Z}_p$ is bigger or equal to the Noether number of all its subrepresentations. In particular, the Noether number of the regular representation is the supremum of the Noether numbers of all indecomposable representations. If this property were true for an arbitrary cyclic p-group, which is a very natural thing to expect in our view, then Corollary 6 would imply that the conjecture is true.

2 Coinvariants of cyclic p-groups

Let $p > 0$ be a prime number and F be a field of characteristic p. We also let G denote the cyclic group $\mathbf{Z}_{p^r}$ of order p^r, where $r \geq 1$ is an integer. Fix a generator σ of G. There are p^r indecomposable representations $V_1, V_2, \ldots, V_{p^r}$ of G over F, where the action of σ on V_n for $1 \leq n \leq p^r$ is given by a Jordan block of size n with ones on the diagonal. Note that V_{p^r} is the regular representation of G. For rest of the way we assume that $p^{r-1} < n$ because otherwise the order of the Jordan block is strictly less than p^r and hence the action is not faithful. For a reference for these facts we direct the reader to the introduction of the recent article [16]. Let $e_1, e_2, \ldots, e_n$ be the Jordan block basis for V_n with $\sigma(e_i) = e_i + e_{i+1}$ for $1 \leq i \leq n-1$ and $\sigma(e_n) = e_n$. Let $x_1, x_2, \ldots, x_n$ denote the corresponding elements in the dual space V_n^*. We use a graded reverse lexicographic order on $F[V_n] = F[x_1, \ldots, x_n]$ with $x_1 < \cdots < x_n$. Since V_n^* is indecomposable it is isomorphic to V_n. Moreover, $x_1, x_2, \ldots, x_n$ is a Jordan block basis in the reverse order. We have $\sigma^{-1}(x_i) = x_i + x_{i-1}$ for $2 \leq i \leq n$ and $\sigma^{-1}(x_1) = x_1$. For simplicity we use the generator σ^{-1} instead of σ and write σ for the new generator. For $0 \leq i \leq r$, let H^i denote the subgroup of G of order p^i. Note that $\sigma^{p^{r-i}}$ is a generator for H^i. For a polynomial $f \in F[V_n]$ we let $N^i(f) = \prod_{1 \leq l \leq p^i} \sigma^{lp^{r-i}}(f)$. We have $N^i(f) \in F[V_n]^{H^i}$. Also for a polynomial $f \in F[V_n]^{H^i}$, define $\mathrm{Tr}_i^G(f) : F[V_n]^{H^i} \to F[V_n]^G$ given by $\mathrm{Tr}_i^G(f) = \sum_{0 \leq l \leq p^{r-i}-1} \sigma^l(f)$. We write N_j^i for $N^i(x_j)$.

Let $1 \leq k \leq r$ and $1 \leq d \leq n - p^{k-1}$ be two integers. We define $w = k(p-1)-1$ which we use repeatedly in the paper. Consider the product $\prod_{0 \leq i \leq w} N_{j_i}^{r-k}$ with $j_i \in \{d-p+2, \ldots, d\}$ if $p-1 \leq d$ and $j_i \in \{1, \ldots, d\}$ if $d < p-1$. We assume that $j_0 \leq j_1 \leq \cdots \leq j_w$. Since $\sigma(x_{j_i}) = x_{j_i} + x_{j_i-1}$, the leading monomial of $N_{j_i}^{r-k}$ is $x_{j_i}^{p^{r-k}}$. Let

$$m = x_{j_0}^{p^{r-k}} x_{j_1}^{p^{r-k}} \cdots x_{j_w}^{p^{r-k}}$$

denote the leading monomial of $\prod_{0 \leq i \leq w} N_{j_i}^{r-k}$. For $0 \leq i \leq w$, write $i = a_i(p-1) + b_i$, where a_i, b_i are non-negative integers with $0 \leq b_i < p-1$. Define $v_{i,0} = x_{j_i+p^{a_i}}^{p^{r-k}}$ for $1 \leq i \leq w$. Note that $v_{i,0}$ is the leading monomial of $N_{j_i+p^{a_i}}^{r-k}$ and for a non-negative integer t set $v_{i,t} = x_{j_i+p^{a_i}-t}^{p^{r-k}}$ if $j_i + p^{a_i} - t \geq 1$ and $v_{i,t} = 0$, otherwise. For a $k(p-1)$-tuple $\alpha = [\alpha(0), \alpha(1), \ldots, \alpha(w)] \in \mathbb{N}^{k(p-1)}$, define

$$v_\alpha = \prod_{0 \leq i \leq w} v_{i,\alpha(i)}.$$

Notice that we have

$$m = \prod_{0 \leq i \leq p-2} v_{i,1} \prod_{p-1 \leq i \leq 2p-3} v_{i,p} \cdots \prod_{(k-1)(p-1) \leq i \leq w} v_{i,p^{k-1}} = v_{\alpha'},$$

where α' denotes the $k(p-1)$-tuple such that

$$\alpha'(i) = p^{a_i} \quad \text{for } 0 \leq i \leq w.$$

We note a couple of well known facts that we use in our computations.

Lemma 1 i) *Let a be a positive integer. Then* $\sum_{0\leq l\leq p-1} l^a \equiv -1 \mod p$ *if $p-1$ divides a and* $\sum_{0\leq l\leq p-1} l^a \equiv 0 \mod p$*, otherwise.*

ii) *Let s, t be integers with base p expansions $t = c_m p^m + c_{m-1}p^{m-1} + \cdots + c_0$ and $s = d_m p^m + d_{m-1}p^{m-1} + \cdots + d_0$, where $0 \leq c_i, d_i \leq p-1$ for $1 \leq i \leq m$. Then* $\binom{t}{s} \equiv \prod_{0\leq i\leq m} \binom{c_i}{d_i} \mod p$.

Proof We direct the reader to [3, 9.4] for a proof of the first statement and to [6] for a proof of the second statement. □

Let I_{d-p+2} denote the ideal in $F[V_n]$ generated by $x_1, \ldots, x_{d-p+1}$ if $d > p-1$ and the zero ideal if $d \leq p-1$. From this point on, all equivalences are modulo I_{d-p+2} unless otherwise stated.

Lemma 2 *For $0 \leq i \leq w$, we have*

$$N^{r-k}_{j_i+p^{a_i}} \equiv v_{i,0} \mod I_{d-p+2}.$$

Proof Since the subgroup of G of order p^{r-k} is generated by σ^{p^k} we have

$$N^{r-k}_{j_i+p^{a_i}} = \prod_{1\leq l\leq p^{r-k}} \sigma^{lp^k}(x_{j_i+p^{a_i}}).$$

Also since $\sigma^j(x_{j_i+p^{a_i}}) = x_{j_i+p^{a_i}} + jx_{j_i+p^{a_i}-1} + \binom{j}{2}x_{j_i+p^{a_i}-2} + \cdots$ for any non-negative integer j, from the previous lemma we get

$$\sigma^{lp^k}(x_{j_i+p^{a_i}}) = x_{j_i+p^{a_i}} + lx_{j_i+p^{a_i}-p^k} + \binom{l}{2}x_{j_i+p^{a_i}-2p^k} + \cdots.$$

Since $0 \leq i \leq w$, a_i is at most $k-1$ and so $j_i + p^{a_i} - p^k \leq j_i - p + 1 < d - p + 2$. Hence $\sigma^{lp^k}(x_{j_i+p^{a_i}}) \equiv x_{j_i+p^{a_i}} \mod I_{d-p+2}$ giving $N^{r-k}_{j_i+p^{a_i}} \equiv x^{p^{r-k}}_{j_i+p^{a_i}} = v_{i,0}$ as desired. □

We now construct a polynomial which is our main tool to bound the top degree of coinvariants. We note that it is a generalization of the polynomials in [7, 3.1] and [11, Proposition 2] to the general $\mathbf{Z}_{p^r}$ case. For a subset $S \subseteq \{0, 1, \ldots, w\}$ let W_S denote the product $\prod_{i\in S} N^{r-k}_{j_i+p^{a_i}}$. We also let S' denote the complement of S in $\{0, \ldots, w\}$. Similarly, let X_S denote the product $\prod_{i\in S} v_{i,0}$. Define

$$T = \sum_{S\subseteq\{0,1,\ldots,w\}} (-1)^{|S|} W_{S'} \operatorname{Tr}^G_{r-k}(W_S).$$

We prove that the leading monomial of T is m. We first show T can be written as a combination of v_α's modulo the ideal I_{d-p+2} such that $\alpha(i) \geq 1$ for $0 \leq i \leq w$.

Lemma 3 *We have*

$$T \equiv \sum_{\alpha\in\mathbb{N}^{k(p-1)}_{\geq 1}} c_\alpha v_\alpha \mod I_{d-p+2},$$

where

$$c_\alpha = \sum_{0\leq l\leq p^k-1} \left(\prod_{i=0}^{w} \binom{l}{\alpha(i)}\right).$$

Proof We have

$$T = \sum_{0 \le l \le p^k - 1} \left(\sum_{S \subseteq \{0,1,\ldots,w\}} (-1)^{|S|} W_{S'} \sigma^l (W_S) \right).$$

By the previous lemma we have $X_S \equiv W_S$ and $X_{S'} \equiv W_{S'}$. Furthermore, since I_{d-p+2} is closed under the action of σ and σ is a ring homomorphism we get

$$T \equiv \sum_{0 \le l \le p^k - 1} \left(\sum_{S \subseteq \{0,1,\ldots,w\}} (-1)^{|S|} X_{S'} \sigma^l (X_S) \right).$$

We also have

$$\sum_{S \subseteq \{0,1,\ldots,w\}} (-1)^{|S|} X_{S'} \sigma^l (X_S) = \prod_{i=0}^{i=w} (v_{i,0} - \sigma^l (v_{i,0})).$$

But$v_{i,0} - \sigma^l(v_{i,0}) = -l v_{i,1} - \binom{l}{2} v_{i,2} - \binom{l}{3} v_{i,3} - \cdots$. Hence the identity for c_α follows. We also get that v_α does not appear in T if $\alpha(i) = 0$ for some $0 \le i \le w$ because $v_{i,0}$ does not appear in $v_{i,0} - \sigma^l(v_{i,0})$. ◻

Lemma 4 *We have $c_{\alpha'} \neq 0$. Moreover, the leading monomial of T is $v_{\alpha'} = m$.*

Proof Since $v_{\alpha'}$ is a higher ranked monomial than all the monomials in I_{d-p+2}, it suffices to compute c_α for which $v_\alpha \notin I_{d-p+2}$. Pick one such $\alpha \in \mathbb{N}^{k(p-1)}$. Then we have $\alpha(i) < p^{a_i+1}$ for $0 \le i \le w$ because otherwise $j_i + p^{a_i} - \alpha(i) \le j_i - p + 1 < d - p + 2$ and so $v_{i,\alpha(i)} \in I_{d-p+2}$ giving $v_\alpha \in I_{d-p+2}$. Therefore, since a_i is at most $k-1$, we get $\alpha(i) < p^k$. It follows that the base p expansion of $\alpha(i)$ has at most k digits for $0 \le i \le w$. Write $\alpha(i) = \alpha(i)_{k-1} p^{k-1} + \alpha(i)_{k-2} p^{k-2} + \cdots + \alpha(i)_0$ and $l = l_{k-1} p^{k-1} + l_{k-2} p^{k-2} + \cdots + l_0$ for the base p expansions of $\alpha(i)$ and l, where $0 \le l \le p^k - 1$. Using these expansions, the previous lemma yields

$$c_\alpha = \sum_{0 \le l_t \le p-1,\ 0 \le t \le k-1} \left(\prod_{0 \le i \le w} \binom{l_{k-1} p^{k-1} + l_{k-2} p^{k-2} + \cdots}{\alpha(i)_{k-1} p^{k-1} + \alpha(i)_{k-2} p^{k-2} + \cdots} \right).$$

Second part of Lemma 1 gives

$$c_\alpha = \sum_{0 \le l_t \le p-1,\ 0 \le t \le k-1} \left(\prod_{0 \le i \le w} \binom{l_{k-1}}{\alpha(i)_{k-1}} \binom{l_{k-2}}{\alpha(i)_{k-2}} \cdots \binom{l_0}{\alpha(i)_0} \right).$$

Now consider the vector α'. Recall that $\alpha'(i) = p^{a_i}$ for $0 \le i \le w$ by definition. Therefore for each $0 \le t \le k-1$ we have

$$\alpha'(i)_t = \begin{cases} 1 & \text{if } t(p-1) \le i < (t+1)(p-1); \\ 0 & \text{otherwise.} \end{cases}$$

It follows that $\prod_{0 \le i \le w} \binom{l_t}{\alpha'(i)_t} = l_t^{p-1}$ for all $0 \le t \le k-1$. Therefore we get $c_{\alpha'} = \sum_{0 \le l_t \le p-1,\ 0 \le t \le k-1} l_{k-1}^{p-1} l_{k-2}^{p-1} \cdots l_0^{p-1} = (-1)^k \neq 0$ by Lemma 1.

To prove the second statement of the theorem we show that for $\alpha \in \mathbb{N}^{k(p-1)}$ with $c_\alpha \neq 0$ and $v_\alpha \notin I_{d-p+2}$ we have $\alpha(i) \ge \alpha'(i)$ for $0 \le i \le w$. Note that this gives we have either $v_\alpha < v_{\alpha'}$ or $\alpha = \alpha'$, implying $v_{\alpha'}$ is the leading monomial of T as desired. We may assume $k > 1$ because otherwise $\alpha'(i) = 1$ for all $0 \le i \le w = p-2$ and hence $\alpha(i) \ge \alpha'(i)$ for all $0 \le i \le w$ since all coordinates of α are at least one by the previous lemma. Also $\alpha(i) < p^{a_i+1}$ by the first paragraph of the proof so we have $\alpha(i) < p^{k-1}$ for $0 \le i \le (k-1)(p-1)-1$. Hence, $\alpha(i)_{k-1} = 0$ unless $(k-1)(p-1) \le i \le w$. So we can write

$$c_\alpha = \sum_{0 \le l_{k-1} \le p-1} \left(A \prod_{(k-1)(p-1) \le i \le k(p-1)-1} \binom{l_{k-1}}{\alpha(i)_{k-1}} \right),$$

where $A = \sum_{0 \le l_t \le p-1,\ 0 \le t \le k-2} \left(\prod_{0 \le i \le w} \binom{l_{k-2}}{\alpha(i)_{k-2}} \cdots \binom{l_0}{\alpha(i)_0} \right)$. Notice that $\alpha(i)_{k-1}$ is at most one for $(k-1)(p-1) \le i \le w$ because otherwise for one i we would have $j_i + p^{a_i} - \alpha(i) = j_i + p^{k-1} - \alpha(i) \le j_i - p^{k-1}$. But $k > 1$ so $j_i - p^{k-1} < d - p + 2$ and, therefore, $v_{i,\alpha(i)} \in I_{d-p+2}$, giving a contradiction. It follows that $\prod_{(k-1)(p-1) \le i \le w} \binom{l_{k-1}}{\alpha(i)_{k-1}}$, as a polynomial in l_{k-1}, is of degree at most $p-1$. Then from the first part of Lemma 1 it follows that it is of degree $p-1$ and hence $\alpha(i)_{k-1} = 1$ for $(k-1)(p-1) \le i \le w$, giving $\alpha(i) \ge p^{k-1} = \alpha'(i)$ for $(k-1)(p-1) \le i \le w$. We assume that $\alpha(i) \ge \alpha'(i) = p^{a_i}$ (equivalently, $\alpha(i)_{a_i} \ge 1$) for $t(p-1) \le i \le w$ some positive integer $t < k-1$ and proceed with reverse induction on t. Since $\alpha'(i) = 1$ for $0 \le i < p-1$ and $\alpha(i) \ge 1$ for all i, we also assume that $t > 1$. First note that $\alpha(i)_{t-1} = 0$ for $t(p-1) \le i \le w$ because otherwise for that i we would have $\alpha(i) \ge p^{a_i} + p^{t-1}$ and therefore $j_i + p^{a_i} - \alpha(i) \le j_i - p^{t-1} < d - p + 2$ ($t > 1$ is required for the last inequality) giving $v_{i,\alpha(i)} \in I_{d-p+2}$. Moreover, since $\alpha(i) < p^{a_i+1}$ for all i, we have $\alpha(i)_{t-1} = 0$ for $0 \le i \le (t-1)(p-1)-1$. It follows that $\prod_{0 \le i \le w} \binom{l_{t-1}}{\alpha(i)_{t-1}} = \prod_{(t-1)(p-1) \le i \le t(p-1)-1} \binom{l_{t-1}}{\alpha(i)_{t-1}}$. We also have $\alpha(i)_{t-1} \le 1$ for $(t-1)(p-1) \le i \le t(p-1)-1$ because otherwise $j_i + p^{a_i} - \alpha(i) = j_i + p^{t-1} - \alpha(i) \le j_i + p^{t-1} - 2p^{t-1} < d - p + 2$. Furthermore, just as we saw for l_{k-1}, the degree of the polynomial $\prod_{(t-1)(p-1) \le i \le t(p-1)-1} \binom{l_{t-1}}{\alpha(i)_{t-1}}$ should be a multiple of $p-1$ by Lemma 1. But $\alpha(i)_{t-1} \le 1$, so we get $\alpha(i)_{t-1} = 1$ for $(t-1)(p-1) \le i \le t(p-1)-1$. Hence $\alpha(i) \ge p^{t-1} = \alpha'(i)$ for $(t-1)(p-1) \le i \le t(p-1)-1$. This completes the induction and we obtain the second statement of the lemma. □

Theorem 5 *The top degree of coinvariants $F[V_n]_G$ is bounded above by $\frac{(r^2+3r)p^r}{2}$.*

Proof It is a standard fact that for any homogeneous ideal I in $F[V_n]$, the set of monomials that are not in the lead term ideal of I forms a vector space basis for $F[V_n]/I$. Therefore to give a bound on the top degree of $F[V_n]_G$, it suffices to give a bound on the top degree of a monomial in $F[V_n]$ that is not a leading monomial in the Hilbert ideal $F[V_n]^G_+ \cdot F[V_n]$. Let m be a monomial in $F[V_n]$ that is not a leading monomial in $F[V_n]^G_+ \cdot F[V_n]$. Write

$$m = m_1 m_2 \cdots m_r x_n^a,$$

where $m_k \in F[x_{n-p^k+1}, \ldots, x_{n-p^{k-1}}]$ for $1 \le k \le r-1$ and $m_r \in F[x_1, \ldots, x_{n-p^{r-1}}]$. By the previous lemma m is not be divisible by the leading monomial of a product $\prod_{0 \le i \le w} N_{j_i}^{r-k}$ with $j_i \in \{d-p+2, \ldots, d\}$ for any $n - p^k + p - 1 \le d \le n - p^{k-1}$ and $1 \le k \le r-1$ nor by a product $\prod_{0 \le i \le r(p-1)-1} N_{j_i}^0 = \prod_{0 \le i \le r(p-1)-1} x_{j_i}$ with $j_i \in \{\max(1, d-p+2), \ldots, d\}$ for any $1 \le d \le n - p^{r-1}$. Moreover, for $1 \le k \le r-1$ each variable in $\{x_{n-p^k+1}, \ldots, x_{n-p^{k-1}}\}$ can appear with multiplicity of $p^{r-k} - 1$ in m_k without effecting the divisibility by the leading monomial of any $N_{j_i}^{r-k}$. It follows for $1 \le k \le r-1$ that the degree of m_k is at most

$\frac{p^{r-k}k(p-1)(p^k-p^{k-1})}{p-1}+(p^k-p^{k-1})(p^{r-k}-1)$ which is smaller than $(k+1)p^r$. Similarly, the degree of m_r is bounded above by $\frac{r(p-1)(n-p^{r-1})}{p-1}$ which is smaller than rp^r. Finally, since the leading monomial of N_n^r is $x_n^{p^r}$, we get $a < p^r$. Summing these bounds up we get that the degree of m is smaller than $\sum_{k=1}^{r-1}(k+1)p^r + rp^r + p^r = \frac{(r^2+3r)p^r}{2}$. □

It turns out that the bound we obtain for the top degree of coinvariants is also a bound for the degrees of the generators of the invariant ring of the regular representation V_{p^r}.

Corollary 6 *We have* $\beta(V_{p^r}) \leq \frac{(r^2+3r)p^r}{2}$.

Proof We proceed by induction on r and the case $r = 1$ has been settled in [7]. Let $\operatorname{Im}\operatorname{Tr}_0^G$ denote the image of Tr_0^G. By [9, 3.3] we have that $F[V_{p^r}]^G/\operatorname{Im}\operatorname{Tr}_0^G$ is isomorphic to the invariant ring $F[V'_{p^{r-1}}]^{H^{r-1}}$ of the regular representation $V'_{p^{r-1}}$ of the cyclic p-group H^{r-1} of order p^{r-1}, where the isomorphism scales the degrees by $1/p$. Hence it follows by induction that $F[V_{p^r}]^G/\operatorname{Im}\operatorname{Tr}_0^G$ is generated as an algebra by invariants up to degree $\frac{(r^2+r-2)p^r}{2}$. On the other hand, as we outlined in the introduction, the top degree of $F[V_{p^r}]_G$ is an upper bound for the degree of a polynomial in $\operatorname{Im}\operatorname{Tr}_0^G$ that is not expressible by invariants of strictly smaller degree. Hence from the previous theorem we get $\beta(V_{p^r}) \leq \max(\frac{(r^2+3r)p^r}{2}, \frac{(r^2+r-2)p^r}{2}) = \frac{(r^2+3r)p^r}{2}$ as desired. □

References

1. Campbell, H.E.A., Fodden, B., Wehlau, D.L.: Invariants of the diagonal C_p-action on V_3. J. Algebra **303**(2), 501–513 (2006)
2. Campbell, H.E.A., Hughes, I.P.: Vector invariants of $U_2(\mathbf{F}_p)$: a proof of a conjecture of Richman. Adv. Math **126**(1), 1–20 (1997)
3. Campbell, H.E.A., Hughes, I.P., Shank, R.J., Wehlau, D.L.: Bases for rings of coinvariants. Transform. Groups **1**(4), 307–336 (1996)
4. Campbell, H.E.A., Shank, R.J., Wehlau, D.L.: Vector invariants for the two-dimensional modular representation of a cyclic group of prime order. Adv. Math **225**(2), 1069–1094 (1996)
5. Dickson, L.E.: On invariants and the theory of numbers. Dover Publications Inc., New York (1966, reprint)
6. Fine, N.J.: Binomial coefficients modulo a prime. Amer. Math. Monthly **54**, 589–592 (1947)
7. Fleischmann, P., Sezer, M., Shank, R.J., Woodcock, C.F.: The Noether numbers for cyclic groups of prime order. Adv. Math **207**(1), 149–155 (2006)
8. Fleischmann, P.: The Noether bound in invariant theory of finite groups. Adv. Math **156**(1), 23–32 (2000)
9. Fleischmann, P., Kemper, G., Shank, R.J.: On the depth of cohomology modules. Q. J. Math **55**(2), 167–184 (2004)
10. Fogarty, J.: On Noether's bound for polynomial invariants of a finite group. Electron. Res. Announc. Amer. Math. Soc. **7**:5–7 (2001) (electronic)
11. Neusel, M.D., Sezer, M.: The invariants of modular indecomposable representations of Z_{p^2}. Math. Ann **341**(3), 575–587 (2008)
12. Noether, E.: Der endlichkeitssatz der invarianten endlicher gruppen. Nachr. Ges. Wiss. Gttingen 89–92 (1916) (reprinted in: Collected Papers, Springer, Berlin, pp. 181–184 (1983))
13. Richman, D.R.: Invariants of finite groups over fields of characteristic p. Adv. Math **124**(1), 25–48 (1996)
14. Shank, R.J.: S.A.G.B.I. bases for rings of formal modular seminvariants [semi-invariants]. Comment. Math. Helv **73**(4), 548–565 (1998)
15. Shank, R.J., Wehlau, D.L.: Noether numbers for subrepresentations of cyclic groups of prime order. Bull. London Math. Soc **34**(4), 438–450 (2002)
16. Shank, R.J., Wehlau, D.L.: Decomposing symmetric powers of certain modular representations of cyclic groups. In: Symmetry and spaces. Progress in Mathematics, vol. 278, pp. 169–196. Birkhäuser Boston Inc., Boston (2010)

17. Symonds, P.: On the Castelnuovo–Mumford regularity of rings of polynomial invariants. Ann. of Math (2) **174**(1), 499–517 (2011)
18. Wehlau, D.L.: Invariants for the modular cyclic group of prime order via classical invariant theory. J. Eur. Math. Soc. (2012, in press)